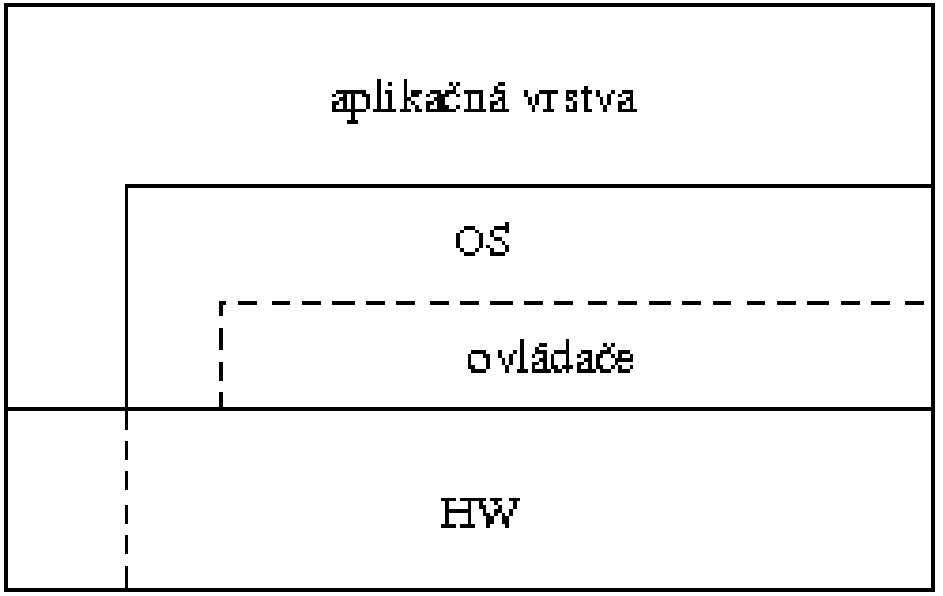
Tento materiál je určený ako podporný študijný materiál na prípravu na skúšku z predmetu Úvod do informačnej bezpečnosti pre študentov Fakulty matematiky, fyziky a informatiky Univerzity Komenského v Bratislave. Na tento účel si študent môže vytvoriť elektronickú aj tlačenú kópiu tohto materiálu.

Bezpečnosť operačných systémov

RNDr. Jaroslav Janáček
KI FMFI UK

Vrstvy informačného systému

- aplikačná vrstva
  - klient
  - server
- (databázová vrstva)
- operačný systém
- hardvér
- prostredie
  - sieť
  - priestory, ľudia



Funkcie vrstiev

- poskytovanie služieb vyšším vrstvám
  - abstrakcia nižších vrstiev
- izolácia vyšších vrstiev od nižších
  - dôležitý predpoklad pre účinnú implementáciu mechanizmov
  - nie vždy úplná
    - napr. aplikácia priamo používa časť CPU

Kde implementovať mechnizmy?

- Základný predpoklad účinnosti
  - mechanizmus nesmie byť možné obísť
- Závisí od vrstvy útočníka
  - ťažko sa chráni proti útokom zdola
    - čiastočná výnimka – kryptografia
- Dole sa ťažko formulujú požiadavky zhora
  - pre procesor sú dáta dáta – pre aplikáciu majú dáta štruktúru a sémantiku (význam)

Kde implementovať mechnizmy?

- aplikačná vrstva
  - ochrana proti útokom prostredníctvom aplikácie
  - nepomôže proti útokom na úrovni OS
- hardvér
  - príliš nízko pre aplikačné bezpečnostné problémy
  - nutný pre ochranu OS
- OS
  - ochrana dát
  - ochrana aplikácií

Bezpečnostné funkcie OS

- Identifikácia a autentifikácia používateľov
- Riadenie prístupu k prostriedkom
  - voliteľné riadenie prístupu (discretionary access control, DAC)
  - povinné riadenie prístupu (manadatory access control, MAC)
- Separácia aplikácií
  - obmedzenie vzájomného ovplyvňovania sa
- Ochrana systému a hardvéru

Identifikácia a autentifikácia

- identifikácia – používateľské mená
- autentifikácia
  - heslá
    - kvalita hesiel
    - ochrana komunikačného kanála
  - kryptografické prostriedky
    - ssh
    - Kerberos
- single sign on

Seprarácia aplikácií

- oddelenie aplikácií
  - samostatné adresné priestory
  - medziprocesová komunikáciaä
    - zdieľaná pamäť, semafóry, posielanie správ
  - ladiace (debugging) nástroje
- ochrana systému a hardvéru
  - prístup k OS len cez systémové volania
  - privilegované inštrukcie
  - ochrana prístupu do pamäte

Voliteľné riadenie prístupu

- objekty majú vlastníkov
- vlastníci určujú prístupové práva
- bežné v mnohých OS
  - UNIX
  - MS Windows 2000,XP,Vista
  - Novell Netware
- nedostatočné pre ochranu pred inými aplikáciami rovnakého používateľa

Povinné riadenie prístupu

- prístupové práva určené politikou
  - bežné programy ju nemôžu ovplyvniť
- známe zo sveta utajovaných skutočností
  - Bell-LaPadula model – dôvernosť
  - Biba model – integrita
  - objekty a subjekty majú bezpečnostnú úroveň a množinu kategórií
  - $(u_1, M_1) \leq (u_2, M_2) \Leftrightarrow u_1 \leq u_2 \wedge M_1 \subseteq M_2$

Povinné riadenie prístupu

- Bell – LaPadula model
  - subjekt S môže čítať z objektu O ak
    $(u_O, M_O) \leq (u_S, M_S)$ (t.j. zdola)
  - subjekt S môže zapisovať do objektu O ak
    $(u_S, M_S) \leq (u_O, M_O)$ (t.j. hore)
  - zabraňuje „úniku“ tajnejšej informácie do menej tajného objektu
  - dôveryhodné subjekty môžu písať aj „dolu“
    - môžu informáciu „odtajnit“

Povinné riadenie prístupu

- Biba model
  - subjekt S môže čítať z objektu O ak
    $(u_S, M_S) \leq (u_O, M_O)$ (t.j. zhora)
  - subjekt S môže zapisovať do objektu O ak
    $(u_O, M_O) \leq (u_S, M_S)$ (t.j. dolu)
  - zabraňuje ovplyvneniu dôveryhodnejšieho objektu informáciou z nedôveryhodnejšieho objektu
  - dôveryhodné subjekty môžu písať aj „hore“
    - môžu informáciu „zdôveryhodniť“

Povinné riadenie prístupu

- Použiteľnosť Bell-LaPadula a Biba modelov
  - vytvorené pre utajované skutočnosti (Bell-LaPadula)
  - v bežnom prostredí problémy
    - príliš veľa informačných tokov zakázaným smerom
    - príliš veľa subjektov musí byť **dôveryhodných**
    - hrubá granularita dôveryhodnosti subjektov
    - zaslúžia si subjekty „dôveryhodnosť“ ?
      - žiaľ, veľmi nie

Povinné riadenie prístupu

- Domain and Type enforcement (DTE)
  - subjekty pracujú v **doméne**, objekty majú **typ**
  - politika určuje
    - povolené operácie pre doménu a typ
    - prechody medzi doménami
    - typy nových objektov na základe domény subjektu a typu „rodičovského“ objektu
  - SELinux
  - veľmi flexibilné
    - napr. umožňuje aj implementáciu Bell-LaPadula a Biba modelov

Typické bezpečnostné problémy

- chyby v softvéri
  - nedostatočná kontrola vstupov
    - buffer overflow
    - špeciálne znaky
  - race conditions
    - časové okno medzi kontrolou a vykonaním operácie
  - používanie nebezpečných funkcií
    - strcpy, gets, scanf
  - nesprávne používanie funkcií
    - printf (vstup ako formátovací reťazec)

Typické bezpečnostné problémy

- príliš veľké práva programov
  - root (UNIX), system (Windows)
- zneužívanie chýb v programoch na spustenie kódu
  - web browser, e-mail klient, ...
  - bez MAC plný prístup k objektom používateľa
- dôveryhodnosť administrátora
  - neobmedzené práva

Typické bezpečnostné problémy

- nezodpovední používatelia
  - každý používateľ je zodpovedný za bezpečnosť
  - používateľ nechráni len seba, ale aj systém ako celok
- nedostatočná informovanosť o bezpečnosti
  - používatelia
  - administrátori
  - vývojári

Pozor na čiastočné riešenia

- riadenie prístupu
  - prístup priamo k zariadeniu
- šifrovanie, elektronické podpisovanie
  - „odchytenie“ kľúčov, hesiel
- overovanie elektronického podpisu
  - podvrh dôveryhodných verejných kľúčov
- reziduálna informácia
  - disky
  - RAM

Pozor na čiastočné riešenia

- nezabezpečené prístupy k HW
  - PCI, Firewire, CardBus (PCMCIA)

Rady do života

- administrátori
  - minimalizovať dostupnosť systému
  - minimalizovať práva používateľov
  - minimalizovať práva aplikácií
    - najlepšie špeciálny používateľ
  - pravidelne sledovať a aplikovať opravy
  - poučiť používateľov

Rady do života

- používatelia
  - nechať sa poučiť
  - upozorňovať na chyby a neštandardné správanie
  - uvedomiť si svoju zodpovednosť za bezpečnosť
  - používať kvalitné heslá
- vývojári
  - dôkladne poznať používané prostriedky
  - dôkladne kontrolovať vstupy
  - minimalizovať bezpečnostné dopady už v návrhu